(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 July 2002 (11.07.2002)

PCT

(10) International Publication Number
WO 02/054808 A1

(51) International Patent Classification[7]: H04Q 7/32, 7/22, 7/38

(21) International Application Number: PCT/FI01/00347

(22) International Filing Date: 9 April 2001 (09.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20010012 4 January 2001 (04.01.2001) FI

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KÅLL, Jan** [FI/FI]; Jupperinmetsä 2 B, FIN-02730 Espoo (FI). **MUHONEN, Ahti** [FI/FI]; Holperintie 39, FIN-04680 Hirvivaara (FI). **MULLIGAN, Michael** [IE/FI]; Kuninkaankatu 40 B 31, FIN-33200 Tampere (FI).

(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).

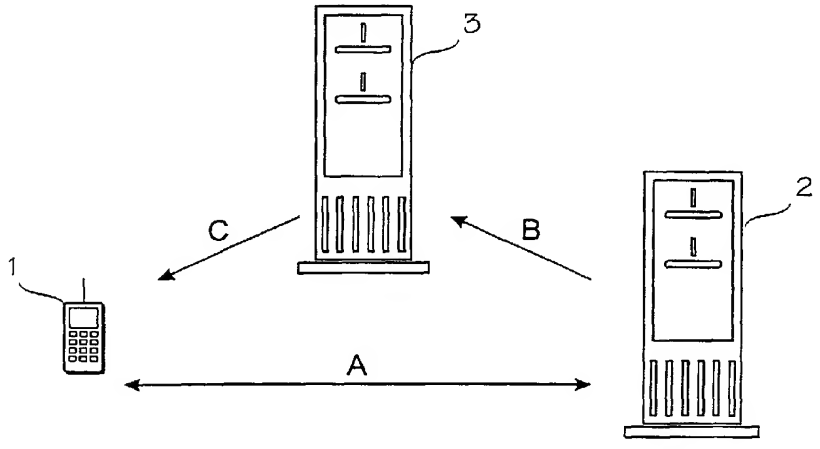
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: A METHOD OF INVOKING PRIVACY



(57) Abstract: The invention relates to a method of invoking privacy related to a user equipment (1) capable of accepting push messages in communications network, which push message is a message a server may send to the user equipment (1) without the user of the user equipment (1) asking for it and the server having the ability to be able to act as a push message initiator. The method comprises the steps of: (i) sending a first request for the personal user data from the user equipment (1) to an origin server (2) over a first channel (A); (ii) the origin server (2) sending a request for personal user data to a supporting server (3); (iii) the supporting server (3) sending a push message over a narrow band channel (C) to the user equipment (1) indicating said request for the user data made by the origin server (2); (iv) the user equipment (1) responding to the push message at least by an allowing message or a disallowing message for the request of data over said narrow band channel; and (v) the supporting server (3) providing the data to the origin server (2) at least partly in response to the allowing message, and rejecting the data providing otherwise.

WO 02/054808 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A METHOD OF INVOKING PRIVACY

FIELD OF THE INVENTION

The present invention relates to communications systems, and more particularly to mechanisms that support privacy invoking. The invention also relates to the use of user data within guidelines such as those outlined by the US FTC (United States Federal Trade Commission).

BACKGROUND OF THE INVENTION

The interaction model of World Wide Web WWW is based on a simple client-server interaction as shown in Figure 1. The client-server relationship can be defined by the relationship between functional entities (for example, managed objects or network layers) in which one entity uses a service provided by another. The user of the service may be called a "client" and the provider of the service may be called a "server". The term interaction can be described as a situation that occurs when one service affects the operation of the other service.

The basis of WWW interaction is that the client requests a resource from the server based on a uniform resource identifier (URI), e.g. uniform resource locator (URL). This identifier individualizes both a file or a directory in the Internet and a protocol needed to use them. Based on this interaction model the server is able to provide some service to the client.

In the process of this interaction the server will often require data from the client. Such data may include the client's PKI (Public Key Infrastructure) Digital Certificate, or perhaps some details about the user on whose behalf the client makes the requests (e.g. username, password, users address).

Due to various constraints in the wireless world the interaction model differs from the model described above. In the wireless model an additional server is introduced to distribute the load across the network. This interaction model is shown in Figure 2. Instead of making the request of the client directly via the link A, the origin server can request information about the client off the supporting server via the link B.

These supporting servers have many uses. Some examples are:

- gathering location data about the user (Location Servers);
- storing and distributing of identity certificates on behalf of the user (Certificate Servers);

- describing the attributes of a user's terminal (User Agent Profile Server); and

- acting as repositories of data.

For various reasons (including legislative) it is considered that personal data should be distributed within strict guidelines. In recent years there has been growing concern about users' privacy on the Internet. This has lead to various guidelines and directives from organizations like OECD (Organization for Economic Co-operation and development) and EU (European Union). The guidelines although quite similar from the various sources are well summed up by the US FTC (United States Federal Trade Commission) Fair Information Practices (FIP) in the Electronic Marketplace. The FIP recommends that users' privacy should follow the 4 following guidelines (http://www.ftc.gov/privacy/index.html):

• Notice – A user should be notified what personal data is used, who is using it, and how it is used;

• Choice – A user should have a choice as to whether or not to allow that use;

• Access – A User should have access to that data where ever it is used; and

• Security – User data should be protected at all times using reasonable security precautions.

The World-Wide-Web Consortium (W3C) has defined a mechanism for terminals to determine the conditions under which personal information may be transmitted to applications. The mechanism is called P3P (Patform for Privacy Preferences. It is actually a framework for:

• defining privacy policy on application servers (i.e. specifying formally what information is gathered and how it is used);

• defining how clients may define their own privacy preferences; and

• how privacy policies may be compared.

P3P does not prescribe specific implementations (beyond relying upon XML (Extensible Markup Language) for defining the policies), but several prototype systems provide the following functions:

• alerting the user each time a WWW site is accessed whose policy differs from the user preferences; and

• requesting the user to authorize the transmission of personal information to the WWW-site.

There exist two state of the art methods for accessing control to user data. A very common access control method is that of using black/white list to control the access to a resource. A black list is a list of entities not allowed to access the resource. If the black list exists all entities are allowed to access the list except those on the black list. A white list is the list of entities allowed to access the resource. If the white list exists no entities are allowed to access the list except those on the white list.

Although this is a rather simple way to provide the level of privacy protection there are some drawbacks, reasons why the method is not applicable to support privacy invoking within guidelines. It is a static method and it has no way of dynamically dealing with data requests. Supposing the user wishes to visit the origin server. The steps they would have to go through are as follows:

1) First they would have to determine what data the origin server may require;

2) Then they would have to go to the appropriate supporting server (or servers as there may be several involved);

3) Then they can proceed to the origin server in order to be served.

Furthermore, there is only the possibility of black or white lists. There is no capability of having a "grey" list where the user is queried to see if they wish to allow the origin server have the data.

Another possibility for accessing control is a method in which the origin server assembles a set of the data it requires and presents it as a list for the client to digitally sign. The origin server then presents this digitally signed list to the supporting server when requesting the personal user data. This method would however involve extra round trips and cryptographic processing on the client. It was precisely these problems that required the use of supporting servers. In other words this scheme would negate the advantage of supporting servers.

The scheme relies on PKI which in turn requires digital certificates. As the digital certificate itself can contain personal user data the simple fact of using the digital certificate could in itself compromise user privacy.

Partially due to the fact that "Privacy" as such is a new area there has been no efforts made in the standards which refer to supporting servers to address the privacy issue. It can clearly be seen from the above use cases

that the data contained on supporting servers is personal user data, and that data should be used in accordance with the appropriate privacy guidelines.

One of the problems associated with the above mentioned current situation is that privacy has not been addressed in wireless Internet standards. Thus there is no defined nor implemented method for supporting servers to protect the privacy wishes of users. Currently the situation with supporting servers is that there is no intervention on behalf of the user when the supporting server receives the request for information. This means that there is no way for the user to receive notice or make a choice with regards to her/his own personal data.

BRIEF DESCRIPTION OF THE INVENTION

It is thus an object of the present invention to provide a new mechanism for supporting privacy invoking in communications systems. The object of the invention is achieved by a method and an arrangement which are characterized by what is stated in the independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

The invention is based on the idea of using a narrow band push channel from a supporting server to a client in order to inform the client about a request for personal data which the supporting server is in possession of. The user can then respond to this request stating whether s/he wishes to allow this request or not.

It is an advantage of the method and the arrangement of the invention that they allow the user to have a choice over whether their personal data is used or not.

Another advantage of the method and the arrangement of the invention is that no previous relationship between the origin server and the supporting server it required.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following the invention will be described in greater detail by means of preferred embodiments with reference to the accompanying drawings, in which

Figure 1 illustrates a prior art WWW interaction model;

Figure 2 illustrates a prior art wireless Internet interaction model; and

Figure 3 shows a privacy protection in supporting server according

to the invention.

DETAILED DESCRIPTION OF THE INVENTION

A general system chart of a communications system to which the invention can be applied may comprise a user equipment that can be a conventional mobile station equipped with a short message service. Although in the following the invention will be described by means of a short message, a short message service, a WAP (Wireless Application Protocol) message and a WAP message service, a message can comprise e.g. at least one of the following messages: a short message, an instant message, an e-mail message, a multimedia message, a unified messaging message, a WAP message or a SIP (Session Initiation Protocol) message. The mobile station can also be mobile station equipped with e.g. an instant message, an e-mail message, a multimedia message, a unified messaging message or a SIP (Session Initiation Protocol) message service.

The basic principles of the invention can be employed to enable privacy invoking between and/or within any mobile communications systems, such as GSM, GPRS, TETRA and UMTS.

The invention may affect some of the elements of an end-to-end system for wireless applications. In the privacy invoking system a client element (referred to a client later on in this application) can be described to be any element which has the ability to receive and handle push messages. One client element can be a typical mobile WAP terminal equipped with this ability.

Supporting repository server element (referred to a supporting server later on in this application) can be described to be any element which has the ability to send push messages to the client, triggered by requests for delivering personal information to other servers. One such supporting server can be a typical server equipped with this ability.

In other words, in order to implement the invention and its embodiments terminals would need to be capable of accepting push messages and the supporting server would require the ability to be able to act as a push initiator. In addition some procedural logic would be required in the terminal and the supporting server.

The narrow band push channel may be defined as a channel over which data or signaling can be sent by a server e.g. without a prior request

received from a client. An example on this kind of a channel is a SMS (Short Message System) channel. Currently SMS may be seen as a unique feature within the wireless world though it's popularity is leading to it being replicated in the broader Internet. Also other types of channels, which are built on asynchronous transfer of data (i.e. not request/response) may be considered a push channel.

The invention proposes the use of a narrow band push channel from the supporting server to the client in order to inform the client about a request for personal data which the supporting server is in possession of. The user can then respond to this request stating whether s/he wishes to allow this request or not. The invention thus proposes to exploit this push channel to protect users' privacy and provide better fulfillment of appropriate privacy directives.

In Figure 3 there is an extra link drawn between the supporting server and the client. This link, link C, is called the push channel link. The sequence of data flows when using the push channel link may be as follows:

1) The client 1 makes the request for the resource to the origin server 2 over a first channel (A);

2) The origin server 2 make the request to the supporting server 3 requesting some personal user data;

3) The supporting server 3 sends a push message over the narrow band channel (C) indicating that the origin server 2 has made the request for the data; (This step is related to the FTC guideline regarding Notice and personal data.)

4) The client 1 responds to the push allowing or disallowing the request for data. (This step is related to the FTC guideline regarding Choice and personal data.) The response may be a simple yes/no. Alternatively the client 1 and the supporting server 3 may negotiate on what data is given and for what purposes; and

5) Depending on the client's 1 response the supporting server 3 will either deliver the data to the origin server 2 or refuse to deliver the data to the origin server 2.

The data which the origin server needs requires processing power on the client which the client does not have. In this case the supporting server supplies the required processing power.

There are many ways of implementing the above-mentioned mechanism. Two alternatives may include the implementation of the invention as an SMS implementation or as a WAP Push implementation.

In an SMS implementation the supporting server would need to support an interface to an SMSC (Short Message Service Center). When the request for personal data arrives from the origin server the supporting server would send the SMS to the client notifying her/him of the origin server's request. The client can then respond indicating her/his preference for the supporting server to accept or reject the origin server's request. The exact content of the SMS messages can be for example a small implementation detail as described above:

1) Supporting Server → Client: " MyBank at www.mybank.com requests your location. Do you wish to give it to them? YES/NO".

2) Client → Supporting Server: "YES"

In a WAP system there is defined a Push framework [Push]. The framework defines 3 components: a Push Client, a Push Initiator PI and a Push Proxy Gateway PPG. Within this implementation the wireless client is also the Push Client capable of receiving WAP Push messages. The Supporting Server in this case acts as the Push Initiator, creating the Push message for delivery to the client. In between the 2 entities there is an entity known as the PPG. The PPG's role is to handle the addressing and delivery of the Push message from PI to the Push Client.

Also in this implementation the exact format of the messages to be passed can be determined but the general procedure would be for the supporting server PI to compose the Push message detailing the origin server's request for personal data. The client would then respond to the message indicating their privacy preferences with regard to the origin servers request.

As described above, the core idea of the invention is the use of the push narrow band channel to alert the user to the use and/or trying to use of their personal data. The response from the user may simply be a simple yes/no response indicating the user's acceptance of the origin server request for the personal data. The response may also be some other type response if it can be read in the supporting server.

However it is also possible that the push message can initiate a pull session allowing the user to negotiate which information they may wish to

divulge. In the pull session the client may request data and the data may be returned on a pull channel. For example, if the origin server requests username and credit card details, the user could respond indicating s/he only wishes to divulge her/his name.

As described above the invention may be applied within the WAP system. One reason for this is the fact that supporting servers are well defined within the architecture of WAP being generally at the forefront of standardisation of the wireless Internet. However the scope of this invention is beyond the scope of the WAP system and architecture and the principle of supporting servers extends beyond the WAP architecture. For example, Location Servers are to be found in 3G (3rd Generation) environments regardless of whether that environment is a WAP environment. The use of certificate URI's is also being extended to the traditional web model. The transmission of user agent profiles is based on W3C work on CC/PP (Composite Capability/Preferences Profiles). In fact the deployment of supporting servers makes sense in any network where there is a wish to make efficient use of bandwidth.

Some of the supporting servers in WAP are described below:

Certificate Server [WPKI, Wireless Public Key Infrastructure].

As a part of the secure handshake in the Internet security protocol SSL/TLS (Secure Sockets Layer/Transport Layer Security) the client and the server may exchange PKI Digital Identity Certificates in order to authenticate each other. The exchange of these certificates can require relatively large bandwidth in a wireless network. For this reason the wireless equivalent of SSL/TLS, WTLS (Wireless Transport Layer Security) allows for a certificate URI to be sent in place of the certificate. This allows for the origin server to retrieve the client's identity certificate from another location on the network (i.e. the supporting server for certificates).

UAProf Server [UAProf].

One of the characteristics of wireless clients is that their characteristics and form factors are vastly different. This is not the case with the WWW, where clients are relatively homogenous. WAP has defined a specification known as UAProf (User Agent Profile) which allows the client to transmit its characteristics to the origin server. Due to bandwidth considerations the client may also transmit the URI which points to the supporting server that contains details of the client's characteristics.

Location Server [Location].

One unique aspect of the mobile Internet is that physical location is a relevant data value. One method of determining the client's physical location relies on measurements being taken by servers in the supporting network. To provide a common abstraction there is defined the Location Server which is the server which can provide information about the client's location. One unique feature of the Location Server is that it does essentially not even need the client's interaction to be of use. The origin server may simply ask the Location Server for the user's location. This type of interaction is particularly sensitive with regards to user privacy issues.

Although each of the supporting servers provide different functionality there are some commonalties between them. In each case:

- the origin server requires some data from the client (e.g. who are they, where are they, what terminal are they using);
- the client sends an identifier allowing the origin server to query the supporting server for the data;
- the supporting server provides data that in the traditional web model would probably be provided by the client; and
- the data asked for and provided has some particular reference to the user of the client (e.g. the user's identity in a certificate, the user's client characteristics, the user's physical location).

The invention assumes that there is a way to associate the MSISDN (Integrated Services Digital Network) or fixed IP (Internet Protocol) address of the terminal with the user identification forwarded by the application (whether name & address, cookie, etc) to the repository. One possibility for this is the repository co-located with a wireless gateway, or containing a user database (white pages).

If the user can have several on-going browsing sessions active as in different browser windows, the push message may have to provide an indication of which site is requesting the disclosure of private data. In the case of a background application that requests private information without the prior initiation by the end-user, the situation is substantially similar. The user should be informed about the application that is trying (autonomously) to gather information about her or him.

Whenever the application server, i.e. the origin server requests personal information from the repository, i.e. from the supporting server, the

repository may send the push message to the end-user, i.e. to the client requesting confirmation for the delivery of the personal information to the application.

In the state of the art supporting servers released this information without intervention from the client as was described previously. This means that there was no way for the user to receive notice or make a choice with regards to their own personal data. Although in some cases implementations of supporting servers may have allowed a simple form of black/white listing which ensured that data was only given to selected parties, this method was and is quite static and limited to a predefined select set of origin servers.

One advantage of the invention is that it improves over earlier solutions in that it is dynamic and flexible. There is no requirement for a user to set up preferences with the supporting server(s) prior to visiting the origin server. This process can take place during the user's session with the origin server. However, it should be noted that as an optimisation the supporting server could retain the list of previous user choices as a dynamic black/white list.

The invention allows for gray lists. Instead of just simple black and white lists, it is now possible to have a gray list where entries on the gray list are queried off the user. This can be seen as an improvement on a simple black/white list solution.

Also the user is in control. In other methods the user must inform each and every supporting server that may contain their personal data about their privacy preferences. Using this method the supporting servers ask the user what their preferences are when they need to know what they are.

The mechanism according to the invention saves bandwidth. Other schemes that attempt to allow for interactivity on behalf of the user (such as digital signed requests) consume extra round trips and bandwidth. The mechanism presented here uses minimal extra trips and bandwidth. This is a clear advantage since the bandwidth of the network link between the client and the origin server (shown as link A in Figure 3) may be very low, or the latency of the link may be poor. With the assistance of the invention the network link between the origin server and the supporting server (shown as link B) may be much higher.

The invention requires no previous relationship between the origin server and the supporting server, or the origin server and the user, client. It

also makes use of unique wireless features such as push technology. The invention allows the use of any push channel to communicate directly with the user, not just the signaling channel of a communications network.

The invention and its preferred embodiments do not assume the presence of a privacy preference negotiation framework (such as P3P), although it could be used in that context. The invention does not require entire programs to be downloaded to the terminal in order to perform the negotiation.

The invention differs from P3P in the following way:

- It does not assume that the application server sends the description of its privacy policy to the terminal;
- It does not assume that the terminal stores privacy preferences; and
- It does assume that the notification is carried out on behalf of the client by the repository of personal data.

It differs from the state of the art prototypes and research in the following way:

- It relies upon the wireless infrastructure for requesting and transmitting disclosure authorization from the end-user. Published proposals consider only a wireline Internet / WWW infrastructure; and
- It does not assume that the information is presented as a form that must be filled in by the end-user (or by an automatic form-filling program), but that it is simply requested by applications from repositories containing user information.

It closer mirrors privacy standards. Although it is a new area the W3C does have a privacy standard known as P3P [P3P]. Part of the P3P specification suite is a user privacy preferences language APPEL [APPEL]. APPEL lists 4 possible outcomes when determining whether P3P policies should be accepted. These outcomes are "accept", "reject", "inform", "warn". When translated to supporting servers, this method allows supporting servers to implement the "inform" and "warn" outcomes. This is not possible with e.g. a black/white listing;

The invention relies upon the capabilities of a wireless application infrastructure, and especially push, for requesting and retrieving disclosure authorizations from the end-user. This constitutes a major benefit in the case of non-interactive applications: the user might not have initiated the application (e.g. an automatic WWW crawler trying to compile information from

repositories scattered in the Internet) and might not even be on-line, but s/he will nevertheless be informed of the request for disclosure of personal data via push messages on his mobile phone.

A service platform for wireless applications makes it possible to fine-tune the handling of the disclosure requests, e.g. by rejecting the requests automatically if it is determined that the end-user is not reachable.

Still another advantage of the invention is that is not specifically related only to requests for location information, but the invention covers nearly all personal data e.g. usernames, passwords, credit card details, address, date of birth, i.e. basically anything one might normally fill in on an Internet form.

Using a narrow band push channel deals with 2 of the 4 privacy guidelines, namely Notice and Choice. By receiving the push message the user is *notified* of the request for the use of their private data. They can also respond with to the request stating whether they wish to allow the request or not. This allows the user to have a *choice* over whether their personal data is used in that fashion or not.

It will be obvious to a person skilled in the art that, as the technology advances, the inventive concept can be implemented in various ways. The invention and its embodiments are not limited to the examples described above but may vary within the scope of the claims.

CLAIMS

1. A method of invoking privacy related to a user equipment (1) capable of accepting push messages in communications network, which push message is a message a server may send to the user equipment (1) without the user of the user equipment (1) asking for it and the server having the ability to be able to act as a push message initiator, **characterized** by the steps of:

(i) sending a first request for the personal user data from the user equipment (1) to an origin server (2) over a first channel (A);

(ii) the origin server (2) sending a request for personal user data to a supporting server (3);

(iii) the supporting server (3) sending a push message over a narrow band channel (C) to the user equipment (1) indicating said request for the user data made by the origin server (2);

(iv) the user equipment (1) responding to the push message at least by an allowing message or a disallowing message for the request of data over said narrow band channel; and

(v) the supporting server (3) providing the data to the origin server (2) at least partly in response to the allowing message, and rejecting the data providing otherwise.

2. A method according to claim 1, **characterized** in that prior to the step (v) the user equipment (1) and the supporting server (3) negotiates on what data is provided to the origin server if the user equipment (1) has send an allowing message to the supporting server.

3. A method according to claim 1 or 2, **characterized** in that the user equipment (1) is a WAP equipment in communications network, and that the push message and the allowing message or the disallowing message are routed between the user equipment (1) and the supporting server (3) through a gateway (PPG) and serving nodes of the communications network.

4. A method according to claim 1 or 2, **characterized** in that the user equipment (1) is an equipment equipped with a short message apparatus in communications network, and that the push message and the allowing message or the disallowing message are routed between the user equipment (1) and the supporting server (3) through a center (SMSC) and serving nodes of the communications network.

5. A method according to claims 1 to 4, **characterized** in that the supporting server (3) informs other supporting servers and/or origin server(s) of the communications network that the user has already agreed to reveal information related to her/him so that the origin server(s) need(s) not to send a push message to the user equipment.

6. A method according to any one of claims 1 to 5, **characterized** in that the exchange of push message and allowing or disallowing messages between the user equipment (1) and the supporting server (3) are authorized and/or secured, preferably by methods such as IP sec, the digital signature or Pretty Good Privacy (PGP).

7. A method according to claim 6, **characterized** in that said authorization and/or securing is done by one of the following methods: IP sec, the digital signature or Pretty Good Privacy (PGP).

8. A supporting server in communications network, **characterized** in that it is adapted to

(i) receive a request from the origin server (2) requesting personal user data;

(ii) send a push message over a narrow band channel (C) to the user equipment (1) indicating the request for the data by the origin server (2);

(iii) receive a respond to the push message from the user equipment (1) over said narrow band channel (C) the respond comprising at least an allowing message or a disallowing message for the request of data; and

(iv) provide the data to the origin server (2) at least partly in response to the allowing message, and reject the data providing otherwise.

9. A user equipment, **characterized** in that it is adapted to

(i) send a request for the personal user data to an origin server (2) over a first channel (A);

(ii) receive a push message over a narrow band channel (C) the message indicating the request for the data made by the origin server (2) from a supporting server (3); and

(iii) respond to the push message over said narrow band channel at least by an allowing message or a disallowing message for the request of data.

10. A communications system, **characterized** in that it comprises at least one user equipment according to claim 9 and/or at least one supporting server according to claim 8.

Fig. 1

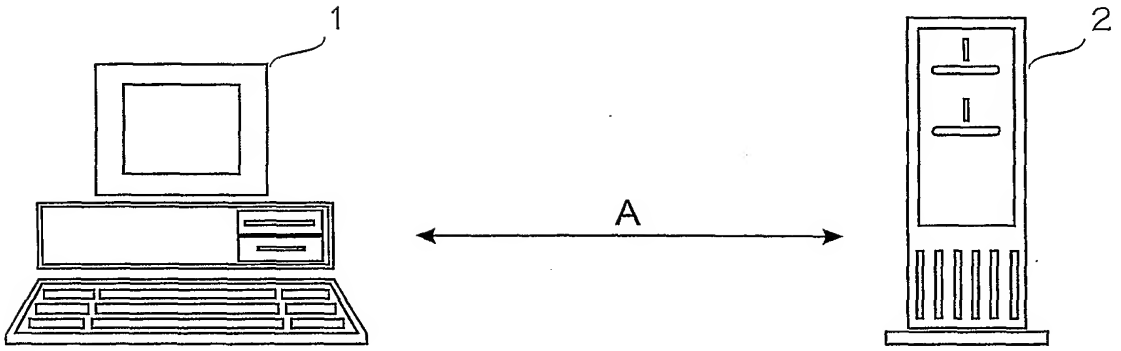


Fig. 2

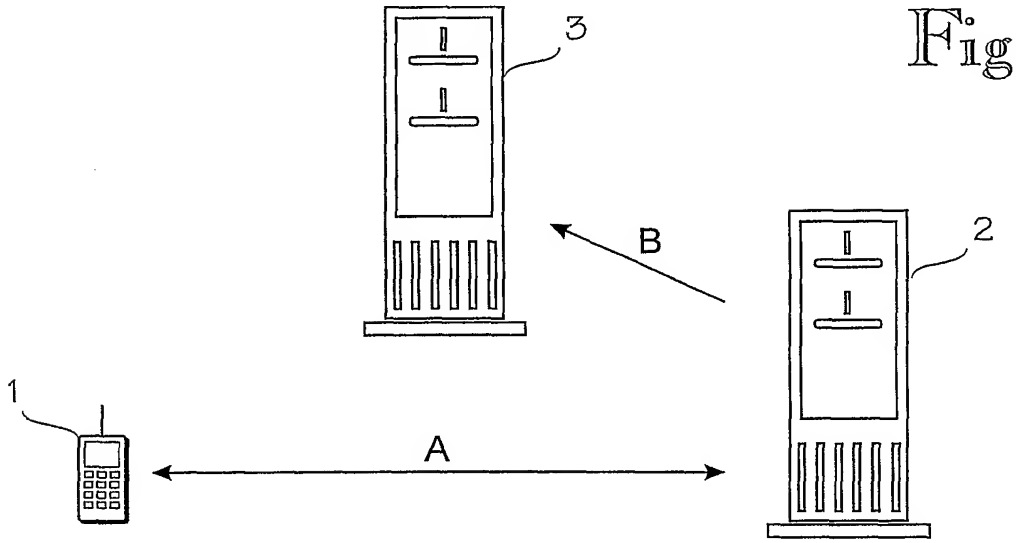
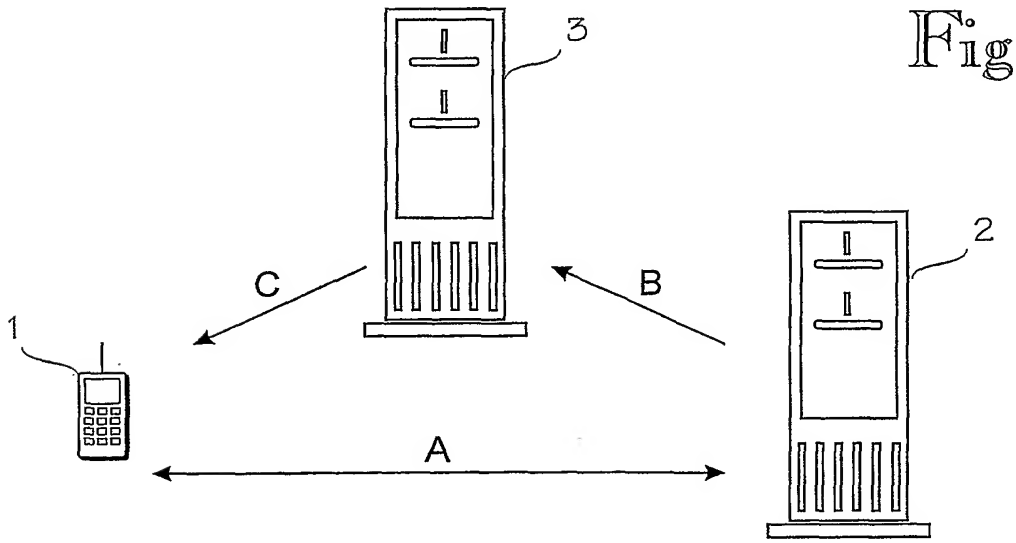


Fig. 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00347

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/32, H04Q 7/22, H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0079811 A1 (SWISSCOM AG), 28 December 2000 (28.12.00), page 4, line 15 - page 8, line 12, abstract ---	1-10
A	WO 0078005 A2 (NOKIA CORPORATION), 21 December 2000 (21.12.00), abstract ---	1-10
A	Computer Security Applications Conference, 1997 "Achieving User Privacy in Mobile Networks" Bob Askwith et al See the whole document --- ---	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 October 2001	22 -10- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Thomas Tholin/JAn Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00347

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0079811 A1	28/12/00	AU 4128799 A	09/01/01
WO 0078005 A2	21/12/00	AU 5488500 A	02/01/01